Faculty of Information and Communication Technology

CHARACTERIZING BOTNET IN P2P NETWORK FOR UDP PROTOCOL

Noor Zuraidin Bin Mohd Safar

2011

BORANG PENGESAHAN STATUS THESIS*

JUDUL: Characterizing Botnet in P2P Network for UDP Protocol

SESI PENGAJIAN: DIS - JUL 2011

Saya NOOR ZURAIDIN BIN MOHD. SAFAR

(HURUF BESAR)

Mengaku membenarkan tesis Sarjana ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

_____	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
_____	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)
_____	TIDAK TERHAD	

(TANDA TANGAN PENULIS)

Alamat Tetap: No. 4A, Pt. Hj. Yusof, Seri Medan Batu Pahat, Johor

Tarikh: 8/6/2011

(TANDA TANGAN PENYELIA)

Dr Mohd Faizal Abdollah

Nama Penyelia

Tarikh: 8/6/11

CATATAN: * Tesis dimaksudkan sebagai Laporan Akhir Projek Sarjana.
** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

CHARACTERIZING BOTNET IN P2P NETWORK FOR UDP PROTOCOL

NOOR ZURAIDIN BIN MOHD SAFAR

A thesis submitted in fulfillment of the requirements for the degree of Master of Computer Science (Internetworkig Technology)

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2011

ABSTRACT

In modern society, an extensive range of business, infrastructure, and human needs, such as communications, utilities, banks, and leisure services are now provided by systems that rely on the secure and efficient operation of computer networks. As networks increase in size and complexity, a thorough understanding of their behavior is crucial to protect them from security threats. One of the threats to the network today is the threat of Botnet. This study will carry out the characterizing botnet in computer networks. In the beginning of the study, botnet architecture, behaviour, topology and mechanism are discussed. To analyze the characteristic, behaviour or pattern of the botnet base on the network traffic, a proper network analyzing tools is needed. Several network analysis tools available today are use for the analysis process of the network traffic. In the analysis phase, the botnet detection strategies base on the signature and DNS anomaly approach are selected to identify the behaviour and the characteristic of the botnet. In anomaly approach most of the behavioral and characteristic identification of the botnet is done by comparing between the normal and abnormal traffic. The main focus of the network analysis is studied on UDP protocol network traffic. Based on the analysis of the network traffic, the following anomalies are identified, abnormal DNS packet request, the NetBIOS attack, abnormal DNS MX query, DNS amplification attack and UDP flood attack. During the analysis process, the irregularity of the network traffic behaviour shows the characteristic of the botnet are existed in the network. The identified characteristic of the botnet can be used for future detection tools and mitigation of the botnet.

ABSTRAK

Pada masa kini dan di dalam masyarakat moden, pelbagai pilihan perniagaan, infrastruktur, dan keperluan manusia, seperti komunikasi, utiliti, bank, dan perkhidmatan rekreasi kini disediakan oleh sistem yang bergantung pada operasi yang selamat dan cekap menggunakan system rangkaian komputer. Dengan peningkatan saiz di dalam rangkaian, pemahaman menyeluruh tentang perilaku rangkaian komputer adalah amat penting untuk melindungi entity tersebut daripada ancaman keselamatan. Salah satu ancaman terhadap rangkaian pada masa kini adalah ancaman Botnet. Penyelidikan ini meragkumi analisa ciri-ciri botnet di dalam rangkaian komputer. Pada awal kajian, strucktur botnet, perilaku, topologi dan mekanisma botnet telah di bincangkan. Untuk menganalisis ciri-ciri, kelakuan atau pola dasar botnet pada lalu lintas rangkaian, peralatan yang bersesuaian amatlah perlu untuk menghasilkan keptusan analisa yang tepat. Penyelidikan ini akan menggunakan beberapa alat analisis rangkaian yang sedia ada pada masa kini. Pada tahap analisis, pendekatan berasaskan *signature* dan *DNS anomaly* telah dipilih untuk mengenalpasti perilaku dan ciri-ciri botnet. Dalam pendekatan anomali, perbandingan perilaku dibuat di antara lalu lintas rangkaian yang normal dan tidak normal. Fokus utama dari analisis rangkaian berdasarkan kepada lalu lintas rangkaian berprotokol UDP. Daripada analisis lalu lintas rangkaian, anomali berikut dikenalpasti, *abnormal DNS packet request*, serangan ke atas protokol NetBIOS, *abnormal DNS MX query*, *DNS amplification attack* dan *UDP flood attack*. Dari hasil analisis, ketidakteraturan perilaku pada lalu lintas rangkaian menunjukkan ciri-ciri botnet telah wujud di dalam rangkaian. Dengan mengenalpasti ciri-ciri dan perilaku botnet ini, ia boleh digunakan untuk pembagunan alat pengesan botnet dan boleh mengurangkan bahaya yang diterbitkan oleh botnet pada masa akan datang.

DEDICATION

To my family for their love, caring, sacrifice, and support.

ACKNOWLEDGEMENT

Alhamdulillah, all praises to Allah, for the strengths and blessing in completing this project. Pursuing a master project is a both painful and enjoyable experience. It is just like climbing a high peak, step by step, accompanied with bitterness, hardships, frustration, encouragement and trust and with so many kinds of people help. When I found myself at the endpoint of the writing, I realized that it was, in fact, teamwork that got me there. Though, it will not be enough to express my gratitude in words to all those people who helped me.

First of all, I would like to give my sincere thanks to my honorific supervisor, Dr. Mohd. Faizal Abdollah, by accepting my project proposal and be my supervisor, without any hesitation when I presented him my project proposal. He offered me so much advice, patiently supervising me, and always guiding me in the right direction. I have learned a lot from him, without his help I could not have finished my work successfully. I would like also to thank the following individuals for their support during the completion of this project, Dr. Abdul Samad Shibghatullah and Dr. Zul Azri Muhamad Noh for the help and insight they offered into this project.

Special thanks are also given to Dean, Faculty of Information and Communication Technology, Professor Dr. Shahrin Sahib @ Sahibuddin and also to the Deputy Dean, Faculty of Information and Communication Technology Associate Professor Dr. Burairah Hussin. Their encouragement and help made me feel confident to fulfill my desire and to overcome every difficulty I encountered.

I also appreciate the help and advice from my friend Ms. Raihana Syahirah Abdullah and UTeM Security Lab technician Mr. Badrolhisham bin Harun . Their help and kind during the entire lab activities, collecting data, setup and configure the network and others are highly appreciated.

Last but not least, my deepest gratitude goes to my wife Fadzlina Hani Samani, my beloved son and daughter, M Syahmi Wafiq and Nur Qistina Faqihah for their support and blessing. Deepest appreciation also goes to my parents Mohd Safar Muliorejo and Sinah Sidal who are never give up on me from the first day of my life till now for their support and encouragement. Lastly, to those who are involved direct or indirectly to my project. Your help is highly appreciated. Thank you.

APPROVAL

I hereby declare that I have read through this project report and in my opinion this project report is sufficient in terms of scope and quality for the award of the degree of Master of Computer Science (Internetworking Technology).

Signature : .....

Supervisor : Dr Mohd Faizal Abdollah

Date : 8/6/11

DECLARATION

I hereby declare that this project report entitled "Characterizing Botnet in P2P Network for UDP Protocol" is the result of my own research except as cited in the references. The report has not been accepted for any degree and is not concurrently submitted in candidature of any other degrees.

Signature : .....

Name : NOOR ZURAIDIN MOHD. SAFAR

Date : 8/6/2011

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CRC	-	Cyclic Redundancy Check
Crontab	-	Cron Table
DDNS	-	Dynamic Domain Name System
DDoS	-	Distributed Denial of Service
DHCP	-	Dynamic Host Configuration Protocol
DNS	-	Domain Name System
DoS	-	Denial of Service
FTP	-	File Transfer Protocol
HTTP	-	Hypertext Transfer Protocol
ICMP	-	Internet Control Message Protocol
IDS	-	Intrusion Detection System
IP	-	Internet Protocol
IPTV	-	Internet Protocol Television
IRC	-	Internet Relay Chat
ISOTF	-	Internet Security Operation Task Force
ISP	-	Internet Service Provider
LAN	-	Local Area Network
libcap	-	Promiscuous Capture Library
MTA	-	Mail Transfer Agent
MUA	-	Mail User Agent
MX	-	Mail Exchanger
MyCERT	-	Malaysian Computer Emergency Response Team
NBNS	-	NetBIOS Name Service
NetBIOS	-	Network Basic Input Output System
P2P	-	Peer to Peer
PC	-	Personal Computer

PCAP	-	Packet Capture
RPC	-	Remote Procedure Call
SMTP	-	Simple Mail Transfer Protocol
SYN	-	Synchronize
TCP	-	Transmission Control Protocol
TFTP	-	Trivial File Transfer Protocol
TLD	-	Top Level Domain
TTL	-	Time To Live
UDP	-	User Datagram Protocol
USB	-	Universal Serial Bus
VoIP	-	Voice over Internet Protocol

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Computer networks are critical to modern society. An extensive range of business, infrastructure, and human needs, such as communications, utilities, banks, and leisure services are now provided by systems that rely on the secure and efficient operation of networks. As networks increase in size and complexity, a thorough understanding of their behaviour is crucial to protect them from security threats. One of the most significant threats to the network today is the threat of Botnets.

Botnet is a network of compromised hosts or bots, under the control of a human attacker known as the Botmaster (Rajab et al., 2006). The Botmaster can issue commands to the bots to perform malicious actions, such as recruiting new bots, launching coordinated distributed denial of service (DDoS) attack against some hosts, stealing sensitive information from the bot machine, sending mass spam emails and other threats (Lu et al., 2008). Thus, botnets have emerged as an enormous threat to the internet community. The major difference between botnets and other security threats is that a Botmaster communicates regularly with the bots either via centralized communication channel or decentralized network.

These bots perform any type of destruction on receiving the commands from the Botmaster. Another threat of botnet is when they are used as distributed supercomputers by attackers wishing to crack cryptographic keys (Gu et al., 2007). It is estimated that more than six million infected computers worldwide are connected to a botnet, with China, the USA, Germany, Spain and France are the top five countries for the number of infected computers. Most owners of infected computers do not know that their computer had been attacked by botnet (Brasso, 2007).

Most of the study related to the botnet threats are the preventive actions from the attack of the botnet, identifying the botnet characteristic, detection and the mitigation of the botnet. Based on the current severity of the botnet, it is very important to develop an agile botnet detector in combating the botnet attack. However, before any tools or mechanism is developed, the characteristic of the botnet need to be emphasized thoroughly.

1.2 Background of study

This study, will focus on the overall background how the botnet works, analyzing the network traffic that suspiciously consist of botnet, study the botnet behaviour by comparing the network traffic analysis before and after the botnet is deployed. The network traffic analysis will determine the variant attack of the peer to peer botnet in User Datagram Protocol (UDP) traffic. The analysis of the network traffic will be use to study the botnet behaviour, topologies, lifecycle events and action or the pattern of the botnet. The result of this study could lead to the development of the botnet detector and a future study of the botnet detection and mitigation process.

1.3 Problem Statement

The aspects of the botnet's life-cycle, from propagation, to command and control, and attacks are all evolving constantly (Bailey et al., 2009), therefore constant study in analyzing botnet

behaviour is needed. The intention of this study is to identify the characteristic of botnet behaviour and pattern. The analysis of the network traffic is base on the UDP protocol.

1.4 Research Questions

The main research questions for this study are given as follows:

1. What is the botnet and how it works?
2. What are network behaviour analysis tools to analyze the network traffic?
3. What are the current botnet detection strategies?
4. What is the different characteristic distinguished between good and bad traffic?

1.5 Research Objectives

The purpose of the proposed work is to identify the characteristic of the botnet. The result of the study can be a key factor to identify botnet behaviour and this will be achieved by pursuing the following main objectives:

1. To study the topology, classification , behaviour of the botnet and to identify the related works in combating botnet base on the passive method through analyzing traffic flow and anomaly signature
2. To identify the botnet characteristic and behaviour from the analysis of the good and bad network traffic through network behaviour analysis tools.
3. To analyze, examine and identify botnet characteristic in attacking victims.

1.6 Research Methodology

The methodology used in this research is an iterative process that involves the study of literature review consists of specifications study by referring to a number of documents and

books that lead to certain ideas to accomplish the task. Furthermore, the analysis of the real network will be done by comparing the good and bad network traffic data. Further explanation of the methodology will discussed in Chapter 3: Research Methodology

1.7 Research Scope

The main activities in this study are base on the following scope:

1. Identify major botnet operation, distribution and control mechanism through available document and existing study
2. Analysis the captured network traffic to identify and understand its pattern and data flow behavior
3. From the analysis, the finding can be used to characterize the botnet topology, behaviour or lifecycle by focusing in UDP protocol in peer to peer network.

1.8 Research Contribution

The successful of the study will contribute in the area of characterizing and preventing of the botnet as conclude in the two major contributions as follows:

1. Presenting the information and finding about botnet capability to harm network users especially in internet data peer to peer network environment.
2. The result of the characterizing the botnet behavior can be used for future works in combating the botnet such as in the development of anti-botnet application.

1.9 Project Report Overview

The project report is divided into five chapters:

Chapter 1, Introduction, this chapter provides a justification and also background information of this research, problem statement, research question, objective, methodology, scope and research contribution.

Chapter 2, Literature Review, this chapter explains about the botnet characteristic, the various type of botnet either falls under centralized or decentralized botnet including peer to peer botnet, current method to identify the botnet and several mechanisms to prevent the botnet. The literature review also explains how the botnet affected the UDP protocol in the network.

Chapter 3, Research Methodology, this chapter discusses the methodology which used to achieve the research objective, including research design, technique in collecting data, research requirement and analysis method to characterize the botnet.

Chapter 4, Implementation, this chapter discusses the implementation phase of normal and abnormal traffic data collection. The data set, software and hardware setup is discussed in this chapter.

Chapter 5, Analysis, this is the main part of the study, where analysis of the collected data is take part to characterize the botnet in UDP. The detection method and behaviour of the botnet is discussed detail in the finding. The characterizing is base on the collected data set by analyzing the signature of the botnet and anomaly approach. In anomaly approach to characterize the botnet, the passive action is used by comparing the normal network traffic and abnormal network traffic

Chapter 6, Summary and Conclusion, this chapter will provide the summary of this research, limitation, conclusion and future works.

1.10 Summary

All types of botnets are one of the big threat to the internet community. This study discussed briefly the emergence of botnets, their organization and architecture and botnet life cycle. The reputed botnet types; the architecture they use and their different characteristic are presented base on the analysis of the network traffic when the peer to peer network is used. The main focus of this study is to analyze the network traffic for the threat of the botnet base on the UDP protocol.